Available online at www.sciencedirect.com
ScienceDirect
Decision Support Systems 42 (2006) 1931 – 1943
Decision Support Systems
www.elsevier.com/locate/dss

A fuzzy decision support system for IT Service Continuity threat assessment

Bartel Van de Walle *, Anne-Francoise Rutkowski

Department of Information Systems and Management, Tilburg University, The Netherlands

Received 11 July 2005; received in revised form 18 January 2006; accepted 10 May 2006
Available online 13 July 2006

Abstract

Using fuzzy relational modeling for preference visualization, the FURIA fuzzy decision support system aims to facilitate preference alignment and group agreement. Findings are presented from a field study on IT Service Continuity threat assessments by IT and business managers that motivate the design and development of the FURIA prototype. The results of a pilot evaluation indicate that groups using FURIA are more satisfied with their decision process, consider the process to be better coordinated and show more agreement with the group decision as compared to groups not using FURIA. Therefore, the results indicate that the prototype performs to expectations.

Keywords: Fuzzy sets; Decision support systems; IT Service Continuity; Threat analysis

1. Introduction

IT Service Continuity (ITSC) management focuses on the continuity of IT services within the organization to provide a pre-determined and agreed level of IT services to support the minimum business requirements following an interruption to the business. ITSC management is typically part of a larger Business Continuity Management (BCM) program, which expands beyond IT to include all business services within an organization. ITSC management allows an organization to identify, assess and take responsibility for managing its risks or threats to IT. The increased attention to ITSC in recent years has led many organizations to list all possible threats and risks to the continuity of their IT services. Ideally, such a list or risk registry is complete and tailored to the organization. A key problem in the construction of this list and the ensuing ITSC management is that the different stakeholders involved – such as staff, customers or shareholders – perceive the impact, likelihood and scope of the threats posed to the IT services in a different way [25].

The research findings reported here result from a field research program conducted within a large multinational organization's IT Service Continuity management division for nearly 2 years. In the course of our research, we were confronted with a lack of alignment between IT and business managers regarding the identification of ITSC risks and preferences for the corresponding mitigation measures. On several occasions, this was leading to significant communication clashes between both groups, provoking lengthy discussions during which no consensus was reached on the

* Corresponding author.
E-mail address: bartel@uvt.nl (B. Van de Walle).

0167-9236/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2006.05.002

importance of the risks nor the measures needed. We have reported elsewhere how the use of Group Support Systems (GSS) technology and decision workshops enabled management to successfully arrive at a fairly comprehensive agreed list of key ITSC risks, including risks that were originally identified by just a few or even single members of one of the stakeholder groups [39,40].

Although the use of GSS technology and methods was perceived as a success, the division's managers remained concerned about the lack of agreement and convergence of the discussion within and among the IT and business groups. It was argued that if members of both groups could assess how close – or how far apart – their individual preferences are at any stage of the discussion, communication would be more effective and agreement would be easier to reach. In response to this concern, we designed and developed FURIA (*Fu*zzy *R*elational *I*ncident *A*nalysis), a prototype fuzzy decision support system allowing individual group members to compare their individual assessment of a decision alternative (such as an ITSC risk) to the assessments of the other group members. At the very core of FURIA is an interactive graphical display visualizing group members' relative preference positions. Earlier research has indeed demonstrated that any person has a fundamental need to evaluate his abilities and opinion by comparing him or herself to others, and this particularly in the absence of clearly defined criteria [18]. When carefully balanced, this process of social comparison contributes to better group decision-making [36].

The main objective of this paper is to present the development and a successful experimental evaluation of FURIA – and in particular its visualization of individual preferences – to address preference alignment problems among group members. Although the actual use of FURIA is context independent, we choose to focus on IT Service Continuity as this provides for the organizational context in which the motivation for the design and development of FURIA was clearly pronounced. We hence introduce IT Service Continuity management and clarify the importance of threats and organizational controls in the following section. The response to a threat and the potential contribution of decision support systems for better threat response decision-making is discussed as well. Section 3 summarizes the mathematical foundations from fuzzy set theory on which the design of FURIA is based, the development of which is presented in Section 4. The experimental evaluation of FURIA is presented in Section 5, and we conclude by summarizing our findings and indicating future research in Section 6.

2. IT Service Continuity management

Business Continuity Management (BCM) can be broadly defined as the management process that is concerned with the continuity or resuming of all critical services upon which the business depends within a predefined time after a disruption. As IT is one of these services, IT Service Continuity (ITSC) management is focused on the continuity of IT and is an important part of the overall BCM process [22] as shown in Fig. 1.

IT Service Continuity management requires an organization to identify, assess and take responsibility for managing its threats to IT, thus enabling it to better understand the environment in which it operates, to decide which threats it wants to prevent from becoming real, and to act positively to protect the interests of all stakeholders, which include employees, customers, shareholders, partners, suppliers, etc. [2,33].

2.1. IT Service Continuity: threats and controls

A threat is defined as any act, entity, event or phenomenon with the potential to harm a person or thing. In other words, a threat is a source of potential harm. Sometimes the word *hazard* or *risk* is used as a synonym for threat. As listed in Table 1, common threat sources can be human, natural or environmental, and threats range from terrorist activities, computer virus attacks and uncontrolled fire, to sabotage by employees.

To counter human threats, intrusion detection tools are becoming more prevalent, and government and industry organizations continuously collect data on security events, thereby improving the ability to realistically assess threats [15]. However, it should be noted that many businesses and governments do not want to draw attention to successful attacks upon their systems for fear of other attacks. Therefore, available statistics about threats are not always complete and might be biased [5,43].

In order for the threat to cause harm, it must find a weakness in the protection of a person or thing that can be accidentally triggered or intentionally exploited. The methodology needed to determine whether vulnerabilities are present varies depending on the nature of the information systems and the phase of the software development lifecycle [14]:

- *Design phase*: The search for vulnerabilities should focus on the organization's security policies, planned security procedures and system requirement definitions, and the vendor's or developer's security product analysis.
- *Implementation phase*: The identification of vulnerabilities should be expanded to include more specific